



IFW

Docket No.: 1232-5362

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicant(s): Satoru WAKAO

Group Art Unit: 2621

Serial No.: 10/815,504

Examiner: TBD

Filed: March 31, 2004

For: IMAGE VERIFICATION APPARATUS  
AND IMAGE VERIFICATION METHOD

**CLAIM TO CONVENTION PRIORITY**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

In the matter of the above-identified application and under the provisions of 35 U.S.C. §119 and 37 C.F.R. §1.55, applicant(s) claim(s) the benefit of the following prior application(s):

Application(s) filed in: Japan

In the name of: Canon Kabushiki Kaisha

Serial No(s): 2003-102327

Filing Date(s): April 4, 2003

☒ Pursuant to the Claim to Priority, applicant(s) submit(s) a duly certified copy of said foreign application.

☐ A duly certified copy of said foreign application is in the file of application Serial No. \_\_\_\_\_, filed \_\_\_\_\_.

Respectfully submitted,  
MORGAN & FINNEGAN, L.L.P.

Dated: June, 22 2004

By:

Joseph A. Calvaruso  
Joseph A. Calvaruso  
Registration No. 28,287

**Correspondence Address:**

MORGAN & FINNEGAN, L.L.P.  
345 Park Avenue  
New York, NY 10154-0053  
(212) 758-4800 Telephone  
(212) 751-6849 Facsimile



Docket No. 1232-5362

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicant(s): Satoru WAKAO

Group Art Unit: 2621

Serial No.: 10/815,504

Examiner: TBD

Filed: March 31, 2004

For: IMAGE VERIFICATION APPARATUS  
AND IMAGE VERIFICATION METHOD

**CERTIFICATE OF MAILING (37 C.F.R. §1.8(A))**

Mail Stop  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

I hereby certify that the attached:

1. Claim to Convention Priority
2. Certified Priority document - Japanese Patent Application  
Serial No. 2003-102327, filed April 4, 2003
3. Return receipt postcard

along with any paper(s) referred to as being attached or enclosed and this Certificate of Mailing are being deposited with the United States Postal Service on date shown below with sufficient postage as first-class mail in an envelope addressed to the: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Respectfully submitted,  
MORGAN & FINNEGAN, L.L.P.

Dated: June, 22 2004

By: Helen Tiger  
Helen Tiger

**Correspondence Address:**

MORGAN & FINNEGAN, L.L.P.  
345 Park Avenue  
New York, NY 10154-0053  
(212) 758-4800 Telephone  
(212) 751-6849 Facsimile

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日                      2 0 0 3 年    4 月    4 日  
Date of Application:

出 願 番 号                      特 願 2 0 0 3 - 1 0 2 3 2 7  
Application Number:

[ST. 10/C]:                      [ J P 2 0 0 3 - 1 0 2 3 2 7 ]

出      願      人                      キヤノン株式会社  
Applicant(s):

2 0 0 4 年    4 月 1 9 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 254143

【提出日】 平成15年 4月 4日

【あて先】 特許庁長官殿

【国際特許分類】 H04N 5/00

【発明の名称】 画像検証装置、画像検証方法、コンピュータプログラム  
、及びコンピュータ読み取り可能な記録媒体

【請求項の数】 16

【発明者】

    【住所又は居所】 東京都大田区下丸子 3 丁目 3 0 番 2 号 キヤノン株式会  
社内

    【氏名】 若尾 聡

【特許出願人】

    【識別番号】 000001007

    【氏名又は名称】 キヤノン株式会社

【代理人】

    【識別番号】 100090273

    【弁理士】

    【氏名又は名称】 國分 孝悦

    【電話番号】 03-3590-8901

【手数料の表示】

    【予納台帳番号】 035493

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

    【包括委任状番号】 9705348

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 画像検証装置、画像検証方法、コンピュータプログラム、及びコンピュータ読み取り可能な記録媒体

【特許請求の範囲】

【請求項 1】 画像ファイルが改変されているか否かを検証する検証手段と

、  
前記画像ファイルが改変されていることを検出した場合、前記画像ファイルの付属情報の表示形態を変更する表示形態変更手段とを有することを特徴とする画像検証装置。

【請求項 2】 前記表示形態変更手段は、前記画像ファイルの付属情報を消去する手段であることを特徴とする請求項 1 に記載の画像検証装置。

【請求項 3】 前記表示形態変更手段は、前記画像ファイルの付属情報に所定の記号を付加する手段であることを特徴とする請求項 1 に記載の画像検証装置。  
。

【請求項 4】 前記付属情報は、前記画像ファイルに関する情報を含むことを特徴とする請求項 1 ～ 3 のいずれか 1 項に記載の画像検証装置。

【請求項 5】 前記付属情報は、前記画像ファイルを生成した装置に関する情報を含むことを特徴とする請求項 1 ～ 4 のいずれか 1 項に記載の画像検証装置。  
。

【請求項 6】 前記検証手段は、共通鍵暗号方式の共通鍵を用いて前記画像ファイルが改変されているか否かを検出する手段であることを特徴とする請求項 1 ～ 5 のいずれか 1 項に記載の画像検証装置。

【請求項 7】 前記検証手段は、公開鍵暗号方式の公開鍵を用いて前記画像ファイルが改変されているか否かを検出する手段であることを特徴とする請求項 1 ～ 5 のいずれか 1 項に記載の画像検証装置。

【請求項 8】 画像ファイルが改変されているか否かを検証する検証工程と

、  
前記画像ファイルが改変されていることを検出した場合、前記画像ファイルの付属情報の表示形態を変更する表示形態変更工程とを有することを特徴とする画

像検証方法。

【請求項 9】 前記表示形態変更工程は、前記画像ファイルの付属情報を消去する工程であることを特徴とする請求項 8 に記載の画像検証方法。

【請求項 10】 前記表示形態変更工程は、前記画像ファイルの付属情報に所定の記号を付加する工程であることを特徴とする請求項 8 に記載の画像検証方法。

【請求項 11】 前記付属情報は、前記画像ファイルに関する情報を含むことを特徴とする請求項 8～10 のいずれか 1 項に記載の画像検証方法。

【請求項 12】 前記付属情報は、前記画像ファイルを生成した装置に関する情報を含むことを特徴とする請求項 8～11 のいずれか 1 項に記載の画像検証方法。

【請求項 13】 前記検証工程は、共通鍵暗号方式の共通鍵を用いて前記画像ファイルが改変されているか否かを検出する手段であることを特徴とする請求項 8～12 のいずれか 1 項に記載の画像検証方法。

【請求項 14】 前記検証工程は、公開鍵暗号方式の公開鍵を用いて前記画像ファイルが改変されているか否かを検出する手段であることを特徴とする請求項 8～12 のいずれか 1 項に記載の画像検証方法。

【請求項 15】 請求項 8～14 のいずれか 1 項に記載の画像検証方法をコンピュータに実行させることを特徴とするコンピュータプログラム。

【請求項 16】 請求項 15 に記載のコンピュータプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、画像ファイルが改変されているか否かを検証する画像検証装置、画像検証方法、コンピュータプログラム、及びコンピュータ読み取り可能な記録媒体に関するものである。

【0002】

【従来の技術】

現在、デジタルカメラなどの撮像装置で生成された画像データの改変を検証するシステムが提案されている（例えば、特許文献 1、2）。

**【0 0 0 3】**

**【特許文献 1】**

米国特許第 5, 4 9 9, 2 9 4 号明細書

**【特許文献 2】**

特開 2 0 0 2 - 2 4 4 9 2 4 号公報

**【0 0 0 4】**

**【発明が解決しようとする課題】**

画像データ及び付属情報（サムネイル画像、撮影日時、シャッター速度、絞り値、ISO 感度、モデル名、製造番号など）を含む画像ファイルが改変ありと判定された場合、付属情報は改変されている可能性がある。

**【0 0 0 5】**

しかしながら、従来のシステムは、改変されている可能性のある付属情報を検証者にわかり易く通知することまで考慮していないという問題があった。

**【0 0 0 6】**

本発明は、このような問題に鑑みてなされたものであり、改変されている可能性のある付属情報を検証者にわかり易く通知できるようにすることを目的とする。

**【0 0 0 7】**

**【課題を解決するための手段】**

本発明における画像検証装置は、画像ファイルが改変されているか否かを検証する検証手段と、前記画像ファイルが改変されていることを検出した場合、前記画像ファイルの付属情報の表示形態を変更する表示形態変更手段とを有することを特徴とする。

**【0 0 0 8】**

本発明における画像検証方法は、画像ファイルが改変されているか否かを検証する検証工程と、前記画像ファイルが改変されていることを検出した場合、前記画像ファイルの付属情報の表示形態を変更する表示形態変更工程とを有すること

を特徴とする。

#### 【0 0 0 9】

##### 【発明の実施の形態】

以下、図面を参照し、本発明の画像検証装置、画像検証方法、コンピュータプログラム、及びコンピュータ読み取り可能な記録媒体の好適な実施の形態について説明する。

#### 【0 0 1 0】

##### [第 1 の実施の形態]

まず、図 1 を参照し、第 1 の実施の形態における画像検証システムの主要な構成要素を説明する。

撮像装置 1 0 A は、撮影者によって撮影された被写体のデジタル画像から M A C (Message Authentication Code) 付き画像ファイルを生成し、生成した M A C 付き画像ファイルをリムーバブルな記録媒体 (メモリカードなど) 又は外部装置の記録媒体に記録する装置である。撮像装置 1 0 A は、デジタルカメラ、デジタルビデオカメラ、カメラ付き携帯電話、スキャナ、コピー機などの装置により実現可能である。

#### 【0 0 1 1】

撮像装置 1 0 B は、撮影者によって撮影された被写体のデジタル画像からデジタル署名付き画像ファイルを生成し、生成したデジタル署名付き画像ファイルをリムーバブルな記録媒体 (メモリカードなど) 又は外部装置の記録媒体に記録する装置である。撮像装置 1 0 B は、撮像装置 1 0 A と同様に、デジタルカメラ、デジタルビデオカメラ、カメラ付き携帯電話、スキャナ、コピー機などの装置により実現可能である。

#### 【0 0 1 2】

画像検証装置 2 0 は、撮像装置 1 0 A で生成された M A C 付き画像ファイル又は撮像装置 1 0 B で生成されたデジタル署名付き画像ファイルが改変されているか否かを検証する機能と、検証した結果を検証者に通知する機能とを有する装置である。また、画像検証装置 2 0 は、M A C 付き画像ファイル又はデジタル署名付き画像ファイルの付属情報 (サムネイル画像、撮影日時、シャッター速度、絞



り値、ISO感度、モデル名、製造番号など）を検証者に通知する機能を有する装置でもある。これらの機能は、画像検証装置 2 0 が画像検証プログラムに従って実現する機能である。

#### 【0 0 1 3】

次に、図 2 のフローチャートを参照し、MAC 付き画像ファイルの生成処理を説明する。

ステップ S 2 0 1：撮像装置 1 0 A は、撮影者からの指示に従って被写体のデジタル画像を撮像する。

#### 【0 0 1 4】

ステップ S 2 0 2：撮像装置 1 0 A は、付属情報（サムネイル画像、撮影日時、シャッター速度、絞り値、ISO感度など）を生成する。

#### 【0 0 1 5】

ステップ S 2 0 3：撮像装置 1 0 A は、撮像されたデジタル画像を撮影者によって選択された画像圧縮方式（ロスレス圧縮、JPEG など）に従って圧縮する。

#### 【0 0 1 6】

ステップ S 2 0 4：撮像装置 1 0 A は、ステップ S 2 0 2 で生成された付属情報及びステップ S 2 0 3 で圧縮されたデジタル画像のハッシュ値（ダイジェストデータともいう）を生成する。つまり、本実施の形態では、付属情報及びデジタル画像を検証対象とする。なお、ハッシュ値を生成するのに必要なハッシュ関数は、MD 5、SHA 1、RIPEMD などがある。

#### 【0 0 1 7】

ステップ S 2 0 5：撮像装置 1 0 A は、ステップ S 2 0 4 で生成されたハッシュ値を MAC に変換する。MAC は、付属情報及びデジタル画像が改変されているか否かを検証するのに必要な情報である。言い換えれば、デジタル画像及び付属情報がオリジナルな情報であるか否かを検証するのに必要な情報である。本実施の形態では、MAC の生成に共通鍵 K c を用いる。共通鍵 K c は、共通鍵暗号方式（暗号鍵と復号鍵とが同じ暗号方式であり、秘密鍵暗号方式、対称鍵暗号方式ともいう）の共通鍵に相当する情報である。共通鍵 K c は、撮像装置 1 0 A 内

に秘密に管理しなければならない情報である。

#### 【0018】

ステップS206：撮像装置10Aは、MAC付き画像ファイルを生成する。MAC付き画像ファイルの構成の一例を図4に示す。領域401は、ステップS202で生成された付属情報を格納する領域である。つまり、画像ファイルに関する情報（サムネイル画像、撮影日時、シャッター速度、絞り値、ISO感度など）、画像ファイルを生成した装置に関する情報（モデル名、製造番号など）を格納する領域である。本実施の形態では、画像ファイルを生成した装置を特定する番号を「製造番号」と呼ぶ。領域402は、ステップS203で圧縮されたデジタル画像を格納する領域である。つまり、オリジナル画像を格納する領域である。領域403は、領域404に存在する検証データの種別を示すマーカを含む。この場合、マーカはMACを示す。領域404は、ステップS205で得られたMACを格納する領域である。なお、領域404は、領域401と領域402との間又は領域401の内部に配置することも可能である。

#### 【0019】

ステップS207：撮像装置10Aは、ステップS206で生成されたMAC付き画像ファイルをリムーバブルな記録媒体（メモリカードなど）又は外部装置の記録媒体に記録する。

#### 【0020】

次に、図3のフローチャートを参照し、デジタル署名付き画像ファイルの生成処理を説明する。

ステップS301：撮像装置10Bは、撮影者からの指示に従って被写体のデジタル画像を撮像する。

#### 【0021】

ステップS302：撮像装置10Bは、付属情報（サムネイル画像、撮影日時、シャッター速度、絞り値、ISO感度など）を生成する。

#### 【0022】

ステップS303：撮像装置10Bは、撮像されたデジタル画像を撮影者によって選択された画像圧縮方式（ロスレス圧縮、JPEGなど）に従って圧縮する

。

### 【0023】

ステップS304：撮像装置10Bは、ステップS302で生成された付属情報及びステップS303で圧縮されたデジタル画像のハッシュ値（ダイジェストデータともいう）を生成する。つまり、本実施の形態では、付属情報及びデジタル画像を検証対象とする。なお、ハッシュ値を生成するのに必要なハッシュ関数は、MD5、SHA1、RIPEMDなどがある。

### 【0024】

ステップS305：撮像装置10Bは、ステップS204で生成されたハッシュ値をデジタル署名に変換する。デジタル署名は、付属情報及びデジタル画像が改変されているか否かを検証するのに必要な情報である。言い換えれば、デジタル画像及び付属情報がオリジナルな情報であるか否かを検証するのに必要な情報である。本実施の形態では、デジタル署名の生成に秘密鍵K<sub>s</sub>を用いる。秘密鍵K<sub>s</sub>は、公開鍵暗号方式（暗号鍵と復号鍵とが異なる暗号方式であり、非対称鍵暗号方式ともいう）の秘密鍵に相当する情報である。秘密鍵K<sub>s</sub>は、撮像装置10B内に秘密に管理しなければならない情報である。

### 【0025】

ステップS306：撮像装置10Bは、デジタル署名付き画像ファイルを生成する。デジタル署名付き画像ファイルの構成の一例を図5に示す。領域501は、ステップS302で生成された付属情報を格納する領域である。つまり、画像ファイルに関する情報（サムネイル画像、撮影日時、シャッター速度、絞り値、ISO感度など）、画像ファイルを生成した装置に関する情報（モデル名、製造番号など）を格納する領域である。領域502は、ステップS303で圧縮されたデジタル画像を格納する領域である。つまり、オリジナル画像を格納する領域である。領域503は、領域504に存在する検証データの種別を示すマークを含む。この場合、マークはデジタル署名を示す。領域504は、ステップS305で得られたデジタル署名を格納する領域である。なお、領域504は、領域501と領域502との間又は領域501の内部に配置することも可能である。

### 【0026】

ステップS307：撮像装置10Bは、ステップS306で生成されたデジタル署名付き画像ファイルをリムーバブルな記録媒体（メモリカードなど）又は外部装置の記録媒体に記録する。

#### 【0027】

次に、図6を参照し、画像検証装置20の主要な構成要素を説明する。

メディア制御部201は、検証者によって選択されたMAC付き画像ファイル又はデジタル署名付き画像ファイルをリムーバブルな記憶媒体202から読み出し、読み出したMAC付き画像ファイル又はデジタル署名付き画像ファイルを内部メモリ205に格納する。リムーバブルな記憶媒体202は、撮像装置10A又は撮像装置10Bに接続できるものであってもよい。

#### 【0028】

通信制御部203は、検証者によって選択されたMAC付き画像ファイル又はデジタル署名付き画像ファイルを外部装置204の記録媒体からネットワークを介して読み出し、読み出したMAC付き画像ファイル又はデジタル署名付き画像ファイルを内部メモリ205に格納する。なお、外部装置204は、撮像装置10Aであっても、撮像装置10Bであってもよい。

#### 【0029】

メモリ206は、MAC付き画像ファイルの改変の検証に必要な共通鍵Kcを記録したメモリである。共通鍵Kcは、撮像装置10Aの共通鍵Kcと同じ鍵であり、画像検証装置20内に秘密に管理しなければならない情報である。第1画像検証部207は、メモリ206内の共通鍵Kcを用いて内部メモリ205内のMAC付き画像ファイルが改変されているか否かを検証する。

#### 【0030】

メモリ208は、デジタル署名付き画像ファイルの改変の検証に必要な公開鍵Kpを記録したメモリである。公開鍵Kpは、秘密鍵Ksに対応する鍵である。つまり、公開鍵Kpは、公開鍵暗号方式の公開鍵に相当する情報であり、秘密に管理する必要のない情報である。第2画像検証部209は、メモリ208内の秘密鍵Ksを用いて内部メモリ205内のデジタル署名付き画像ファイルが改変されているか否かを検証する。

**【 0 0 3 1 】**

メイン制御部 2 1 0 は、プログラムメモリ 2 1 1 に記録された画像検証プログラムを実行するマイクロコンピュータを有する。

**【 0 0 3 2 】**

表示部 2 1 2 は、メイン制御部 2 1 0 が画像検証プログラムに従って生成された一覧画面を表示する。一覧画面の一例を図 8 及び図 9 に示す。図 8 に示す一覧画面は、“MAC”グループ用の一覧画面であり、“MAC”グループに属する全ての MAC 付き画像ファイルの付属情報（サムネイル画像、撮影日時、シャッター速度、絞り値、ISO 感度、モデル名、製造番号など）、ファイル名、サイズ及び検証結果を並べて表示する一覧画面である。また、図 9 に示す一覧画面は、“デジタル署名”グループ用の一覧画面であり、“デジタル署名”グループに属する全てのデジタル署名付き画像ファイルの付属情報（サムネイル画像、撮影日時、シャッター速度、絞り値、ISO 感度、モデル名、製造番号など）、ファイル名、サイズ、検証結果からなる一覧画面もある。

**【 0 0 3 3 】**

操作部 2 1 3 は、検証者の指示を受け付け、受け付けた指示をメイン制御部 2 1 0 に供給する。検証者は、操作部 2 1 3 を操作することにより、画像検証プログラムに MAC 付き画像ファイル又はデジタル署名付き画像ファイルを登録する。また、検証者は、操作部 2 1 3 を操作することにより、画像検証プログラムに検証した欲しい MAC 付き画像ファイル又はデジタル署名付き画像ファイルを選択する。

**【 0 0 3 4 】**

次に、図 7 のフローチャートを参照し、検証者によって選択された一つ以上の画像ファイルを画像検証プログラムに登録する画像登録処理を説明する。画像登録処理は、画像検証装置 2 0 が画像検証プログラムに従って実行する処理である。

**【 0 0 3 5 】**

ステップ S 7 0 1：メイン制御部 2 1 0 は、検証者によって選択された一つ以上の画像ファイルの中から所定の順序に従って 1 つの画像ファイルを選択する。

以下、メイン制御部 2 1 0 によって選択された M A C 付き画像ファイルを「選択画像ファイル」と呼ぶ。なお、検証者がフォルダを選択した場合、メイン制御部 2 1 0 は、そのフォルダ内の全ての画像ファイルを選択したものとして処理を行う。

#### 【0 0 3 6】

ステップ S 7 0 2：メイン制御部 2 1 0 は、選択画像ファイルのオープンを行い、選択画像ファイルのオープンが成功したか否かを判定する。

#### 【0 0 3 7】

ステップ S 7 0 3：メイン制御部 2 1 0 は、選択画像ファイルのオープンに失敗したことを示すメッセージ又は記号を表示部 2 1 2 に表示する。

#### 【0 0 3 8】

ステップ S 7 0 4：メイン制御部 2 1 0 は、選択画像ファイルをリムーバブルな記録媒体 2 0 2 又は外部装置 2 0 4 の記録媒体から内部メモリ 2 0 5 に読み込むために、選択画像ファイルのリードを行う。選択画像ファイルのリードに失敗した場合、メイン制御部 2 1 0 はステップ S 7 0 5 に進む。選択画像ファイルのリードに成功した場合、メイン制御部 2 1 0 はステップ S 7 0 6 に進む。

#### 【0 0 3 9】

ステップ S 7 0 5：メイン制御部 2 1 0 は、選択画像ファイルのリードに失敗したことを示すメッセージ又は記号を表示部 2 1 2 に表示する。

#### 【0 0 4 0】

ステップ S 7 0 6：メイン制御部 2 1 0 は、内部メモリ 2 0 5 内の選択画像ファイルのファイルフォーマットを検査し、選択画像ファイルのファイルフォーマットが正常であるか否かを判定する。

#### 【0 0 4 1】

ステップ S 7 0 7：選択画像ファイルのファイルフォーマットが正常でない場合、メイン制御部 2 1 0 は、内部メモリ 2 0 5 内の選択画像ファイルを破棄するとともに、選択画像ファイルのファイルフォーマットが正常でないことを示すメッセージ又は記号を表示部 2 1 2 に表示する。

#### 【0 0 4 2】

ステップ S 7 0 8 : 選択画像ファイルのファイルフォーマットが正常である場合、メイン制御部 2 1 0 は、選択画像ファイルに検証データ（本実施の形態では、MAC 又はデジタル署名）が付加されているか否かを判定する。

#### 【0 0 4 3】

ステップ S 7 0 9 : 選択画像ファイルに検証データが付加されていない場合、メイン制御部 2 1 0 は、選択画像ファイルを”その他”グループに分類する。”その他”グループは、MAC もデジタル署名も付加されていない画像ファイルからなるグループである。また、メイン制御部 2 1 0 は、選択画像ファイルの付属情報（サムネイル画像、撮影日時、シャッター速度、絞り値、ISO 感度、モデル名、製造番号など）、ファイル名及びサイズを内部メモリ 2 0 5 内の”その他”テーブルに登録する。”その他”テーブルは、”その他”グループに分類された画像ファイルを管理する管理テーブルである。メイン制御部 2 1 0 はさらに、選択画像ファイルのサムネイル画像、ファイル名、撮影日時、シャッター速度、絞り値、ISO 感度、サイズ、モデル名及び製造番号を”その他”グループ用の一覧画面に並べて表示する。なお、選択画像ファイルからサムネイル画像を取り出すことができなかった場合、メイン制御部 2 1 0 は、サムネイル画像を表示する欄にサムネイル画像が存在しないことを示すメッセージ又は記号を表示する。また、メイン制御部 2 1 0 は、一覧画面に”その他”グループに属する画像ファイルの総数を表示する。

#### 【0 0 4 4】

ステップ S 7 1 0 : メイン制御部 2 1 0 は、選択画像ファイルに付加されている検証データの種別を検出する。

#### 【0 0 4 5】

ステップ S 7 1 1 : 選択画像ファイルの検証データがデジタル署名である場合、メイン制御部 2 1 0 は、選択画像ファイルを”デジタル署名”グループに分類する。”デジタル署名”グループは、デジタル署名付き画像ファイルからなるグループである。メイン制御部 2 1 0 は、選択画像ファイルの付属情報（サムネイル画像、撮影日時、シャッター速度、絞り値、ISO 感度、モデル名、製造番号など）、ファイル名及びサイズを内部メモリ 2 0 5 内の”デジタル署名”テーブルに登

録する。”デジタル署名”テーブルは、”デジタル署名”グループに分類された画像ファイルを管理する管理テーブルである。また、メイン制御部 210 は、図 9 に示すように、選択画像ファイルのサムネイル画像、ファイル名、撮影日時、シャッター速度、絞り値、ISO 感度、サイズ、モデル名及び製造番号を”デジタル署名”グループ用の一覧画面に並べて表示する。なお、選択画像ファイルにサムネイル画像が存在しない場合、メイン制御部 210 は、サムネイル画像を表示する欄にサムネイル画像が存在しないことを示すメッセージ又は記号を表示する。また、メイン制御部 210 は、図 9 に示すように、一覧画面に”デジタル署名”グループに属する画像ファイルの総数（本実施の形態では、7）、及び、全てのグループに属する画像ファイルの総数（本実施の形態では、20）を表示する。

#### 【0046】

ステップ S712：選択画像ファイルの検証データが MAC である場合、選択画像ファイルを”MAC”グループに分類する。”MAC”グループは、MAC 付き画像ファイルからなるグループである。メイン制御部 210 は、選択画像ファイルの付属情報（サムネイル画像、撮影日時、シャッター速度、絞り値、ISO 感度、モデル名、製造番号など）、ファイル名及びサイズを内部メモリ 205 内の”MAC”テーブルに登録する。”MAC”テーブルは、”MAC”グループに分類された画像ファイルを管理する管理テーブルである。また、メイン制御部 210 は、図 8 に示すように、選択画像ファイルのサムネイル画像、ファイル名、撮影日時、シャッター速度、絞り値、ISO 感度、サイズ、モデル名及び製造番号を”MAC”グループ用の一覧画面に並べて表示する。なお、選択画像ファイルにサムネイル画像が存在しない場合、メイン制御部 210 は、サムネイル画像を表示する欄にサムネイル画像が存在しないことを示すメッセージ又は記号を表示する。また、メイン制御部 210 は、図 8 に示すように、一覧画面に”MAC”グループに属する画像ファイルの総数（本実施の形態では、10）、及び、全てのグループに属する画像ファイルの総数（本実施の形態では、20）を表示する。

#### 【0047】

ステップ S713：メイン制御部 210 は、検証者によって選択された画像ファイルを全て画像検証プログラムに登録したか否かを判定する。全て検証してい



ない場合、メイン制御部 210 はステップ S701 に戻る。

#### 【0048】

以上の手順により、本実施の形態における画像検証装置 20 は、検証者によって選択された一つ以上の画像ファイルを画像検証プログラムに登録することができる。

#### 【0049】

次に、図 10 のフローチャートを参照し、MAC 署名付き画像ファイルが改変されているか否かを検証する第 1 の画像検証処理を説明する。第 1 の画像検証処理は、画像検証装置 20 が画像検証プログラムに従って実行する処理である。

#### 【0050】

ステップ S1001：検証者は、画像検証プログラムに検証して欲しい一つ以上の MAC 付き画像ファイルを”MAC”グループの中から選択し、図 8 に示す”検証開始”ボタンを押す。メイン制御部 210 は、”検証開始”ボタンが押されたことを検出した後、検証者によって選択された一つ以上の MAC 付き画像ファイルの中から所定の順序に従って一つの MAC 付き画像ファイルを選択する。以下、メイン制御部 210 によって選択された MAC 付き画像ファイルを「選択画像ファイル」と呼ぶ。

#### 【0051】

ステップ S1002：メイン制御部 210 は、選択画像ファイルをリムーバブルな記録媒体 202 又は外部装置 204 の記録媒体から内部メモリ 205 に読み込み、第 1 画像検証部 207 に選択画像ファイルの検証を要求する。第 1 画像検証部 207 は、選択画像ファイルの領域 401 及び領域 402 から付属情報及びデジタル画像を取り出し、それらのハッシュ値を生成する。

#### 【0052】

ステップ S1003：第 1 画像検証部 207 は、選択画像ファイルの領域 404 から MAC を取り出し、メモリ 206 から共通鍵 Kc を読み出す。そして、第 1 画像検証部 207 は、共通鍵 Kc を用いて MAC をハッシュ値に逆変換（復号化）する。

#### 【0053】

ステップ S 1 0 0 4：第 1 画像検証部 2 0 7 は、選択画像ファイルが改変されているか否かを検証するために、ステップ S 1 0 0 2 で得られたハッシュ値とステップ S 1 0 0 3 で得られたハッシュ値とを比較し、二つのハッシュ値が一致するか否かを判定する。選択画像ファイルの領域 4 0 1、領域 4 0 2 及び領域 4 0 4 が全く改変されていない場合、二つのハッシュ値は一致する。二つのハッシュ値が一致した場合、第 1 画像検証部 2 0 7 は、「改変あり」と判定する。言い換えれば、選択画像ファイルがオリジナルであると判定する。選択画像ファイルの領域 4 0 1、領域 4 0 2 及び領域 4 0 4 の少なくとも一つが改変されている場合、二つのハッシュ値は一致しない。二つのハッシュ値が一致しなかった場合、第 1 画像検証部 2 0 7 は、「改変なし」と判定する。言い換えれば、選択画像ファイルがオリジナルでないと判定する。第 1 画像検証部 2 0 7 の判定の結果は、メイン制御部 2 1 0 に通知される。

#### 【 0 0 5 4 】

ステップ S 1 0 0 5：二つのハッシュ値が一致した場合、メイン制御部 2 1 0 は、図 1 2 に示すように、検証結果の欄に「OK」を表示する。OK は、選択画像ファイルが「改変なし」と判定された画像ファイルであることを示す情報である。

#### 【 0 0 5 5 】

ステップ S 1 0 0 6：二つのハッシュ値が一致しなかった場合、メイン制御部 2 1 0 は、メイン制御部 2 1 0 は、図 1 2 に示すように、検証結果の欄に「NG」を表示する。NG は、選択画像ファイルが「改変あり」と判定された画像ファイルであることを示す情報である。選択画像ファイルが「改変あり」と判定された画像ファイルである場合、領域 4 0 1 内の付属情報は改変されている恐れがある。そこで、メイン制御部 2 1 0 は、選択画像ファイルの領域 4 0 1 から得られた付属情報（サムネイル画像、撮影日時、シャッター速度、絞り値、ISO 感度、サイズ、モデル名、製造番号など）が改変されている可能性があることを検証者に知らせるために、付属情報の表示形態を第 1、第 2 又は第 3 の表示形態に変更する。第 1 の表示形態は、サムネイル、撮影日時、シャッター速度、絞り値、ISO 感度、サイズ、モデル名及び製造番号の欄に表示されている情報を全て消

去する表示形態である。第2の表示形態は、図12に示すように、サムネイルの欄に表示されているサムネイル画像に改変されている可能性があることを示す記号（例えば、「×」）を付加し、撮影日時、シャッター速度、絞り値、ISO感度、サイズ、モデル名及び製造番号の欄に表示されている情報を全て消去する表示形態である。第3の表示形態は、サムネイル、撮影日時、シャッター速度、絞り値、ISO感度、サイズ、モデル名及び製造番号の欄に表示されている情報に改変されている可能性があることを示す記号（例えば、「×」）を付加する表示形態である。なお、選択画像ファイルの付属情報が改変されている可能性があることを検証者に知らせることができる表示形態であれば、他の表示形態を表示するように構成することももちろん可能である。

#### 【0056】

ステップS1007：メイン制御部210は、検証者によって選択されたMAC付き画像ファイルを全て検証したか否かを判定する。全て検証していない場合、メイン制御部210はステップS1001に戻る。

#### 【0057】

このような処理手順により、画像検証装置20は、検証者によって選択されたMAC付き画像ファイルが改変されているか否かを検証することができる。

#### 【0058】

次に、図11のフローチャートを参照し、デジタル署名付き画像ファイルが改変されているか否かを検証する第2の画像検証処理を説明する。第2の画像検証処理は、画像検証装置20が画像検証プログラムに従って実行する処理である。

#### 【0059】

ステップS1101：検証者は、画像検証プログラムに検証して欲しい一つ以上のデジタル署名付き画像ファイルを”デジタル署名”グループの中から選択し、図9に示す”検証開始”ボタンを押す。メイン制御部210は、”検証開始”ボタンが押されたことを検出した後、検証者によって選択された一つ以上のデジタル署名付き画像ファイルの中から所定の順序に従って一つのデジタル署名付き画像ファイルを選択する。以下、メイン制御部210によって選択されたデジタル署名付き画像ファイルを「選択画像ファイル」と呼ぶ。

**【0 0 6 0】**

ステップ S 1 1 0 2：メイン制御部 2 1 0 は、選択画像ファイルをリムーバブルな記録媒体 2 0 2 又は外部装置 2 0 4 の記録媒体から内部メモリ 2 0 5 に読み込み、第 2 画像検証部 2 0 9 に選択画像ファイルの検証を要求する。第 2 画像検証部 2 0 9 は、選択画像ファイルの領域 5 0 1 及び領域 5 0 2 から付属情報及びデジタル画像を取り出し、それらのハッシュ値を生成する。

**【0 0 6 1】**

ステップ S 1 1 0 3：第 2 画像検証部 2 0 9 は、選択画像ファイルの領域 5 0 4 からデジタル署名を取り出し、メモリ 2 0 8 から公開鍵 K p を読み出す。そして、第 2 画像検証部 2 0 9 は、公開鍵 K p を用いてデジタル署名をハッシュ値に逆変換（復号化）する。

**【0 0 6 2】**

ステップ S 1 1 0 4：第 2 画像検証部 2 0 9 は、選択画像ファイルが改変されているか否かを検証するために、ステップ S 1 1 0 2 で得られたハッシュ値とステップ S 1 1 0 3 で得られたハッシュ値とを比較し、二つのハッシュ値が一致するか否かを判定する。選択画像ファイルの領域 5 0 1、領域 5 0 2 及び領域 5 0 4 が全く改変されていない場合、二つのハッシュ値は一致する。二つのハッシュ値が一致した場合、メイン制御部 2 1 0 は、「改変あり」と判定する。言い換えれば、選択画像ファイルがオリジナルであると判定する。選択画像ファイルの領域 5 0 1、領域 5 0 2 及び領域 5 0 4 の少なくとも一つが改変されている場合、二つのハッシュ値は一致しない。二つのハッシュ値が一致しなかった場合、メイン制御部 2 1 0 は、「改変なし」と判定する。言い換えれば、選択画像ファイルがオリジナルでないと判定する。第 2 画像検証部 2 0 9 の判定の結果は、メイン制御部 2 1 0 に通知される。

**【0 0 6 3】**

ステップ S 1 1 0 5：二つのハッシュ値が一致した場合、メイン制御部 2 1 0 は、図 1 3 に示すように、検証結果の欄に「OK」を表示する。OK は、選択画像ファイルが「改変なし」と判定された画像ファイルであることを示す情報である。

**【 0 0 6 4 】**

ステップ S 1 1 0 6 : 二つのハッシュ値が一致しなかった場合、メイン制御部 2 1 0 は、メイン制御部 2 1 0 は、図 1 3 に示すように、検証結果の欄に「NG」を表示する。NG は、選択画像ファイルが「改変あり」と判定された画像ファイルであることを示す情報である。選択画像ファイルが「改変あり」と判定された画像ファイルである場合、領域 5 0 1 内の付属情報は改変されている恐れがある。そこで、メイン制御部 2 1 0 は、選択画像ファイルの領域 5 0 1 から得られた付属情報（サムネイル画像、撮影日時、シャッター速度、絞り値、ISO 感度、サイズ、モデル名、製造番号など）が改変されている可能性があることを検証者に知らせるために、付属情報の表示形態を第 1、第 2 又は第 3 の表示形態に変更する。第 1 の表示形態は、サムネイル、撮影日時、シャッター速度、絞り値、ISO 感度、サイズ、モデル名及び製造番号の欄に表示されている情報を全て消去する表示形態である。第 2 の表示形態は、図 1 3 に示すように、サムネイルの欄に表示されているサムネイル画像に改変されている可能性があることを示す記号（例えば、「×」）を付加し、撮影日時、シャッター速度、絞り値、ISO 感度、サイズ、モデル名及び製造番号の欄に表示されている情報を全て消去する表示形態である。第 3 の表示形態は、サムネイル、撮影日時、シャッター速度、絞り値、ISO 感度、サイズ、モデル名及び製造番号の欄に表示されている情報に改変されている可能性があることを示す記号（例えば、「×」）を付加する表示形態である。なお、選択画像ファイルの付属情報が改変されている可能性があることを検証者に知らせることができる表示形態であれば、他の表示形態を表示するように構成することももちろん可能である。

**【 0 0 6 5 】**

ステップ S 1 1 0 7 : メイン制御部 2 1 0 は、検証者によって選択されたデジタル署名付き画像ファイルを全て検証したか否かを判定する。全て検証していない場合、メイン制御部 2 1 0 はステップ S 1 1 0 1 に戻る。

**【 0 0 6 6 】**

このような処理手順により、画像検証装置 2 0 は、検証者によって選択されたデジタル署名付き画像ファイルが改変されているか否かを検証することができる

。

**【 0 0 6 7 】**

このように第 1 の実施の形態における画像検証装置 2 0 によれば、改変ありと判定された M A C 付き画像ファイルの付属情報（サムネイル画像、撮影日時、シャッター速度、絞り値、I S O 感度、サイズ、モデル名、製造番号など）の表示形態を変更することができるので、改変されている可能性のある付属情報を検証者にわかり易く通知することができる。

**【 0 0 6 8 】**

また、第 1 の実施の形態における画像検証装置 2 0 によれば、改変ありと判定されたデジタル署名付き画像ファイルの付属情報（サムネイル画像、撮影日時、シャッター速度、絞り値、I S O 感度、サイズ、モデル名、製造番号など）の表示形態を変更することができるので、改変されている可能性のある付属情報を検証者にわかり易く通知することができる。

**【 0 0 6 9 】****[第 2 の実施の形態]**

第 1 の実施の形態は、M A C 付き画像ファイルの付属情報（サムネイル画像、撮影日時、シャッター速度、絞り値、I S O 感度、サイズ、モデル名、製造番号など）、ファイル名及びサイズを表示する前にその画像ファイルが改変されているか否かを検証し、その検証の結果に従って M A C 付き画像ファイルの付属情報の表示形態を第 1、第 2 又は第 3 の表示形態に変更するように変更することが可能である。

**【 0 0 7 0 】**

同様に、第 1 の実施の形態は、デジタル署名付き画像ファイルの付属情報（サムネイル画像、撮影日時、シャッター速度、絞り値、I S O 感度、サイズ、モデル名、製造番号など）、ファイル名及びサイズを表示する前にその画像ファイルが改変されているか否かを検証し、その検証の結果に従って M A C 付き画像ファイルの付属情報の表示形態を第 1、第 2 又は第 3 の表示形態に変更するように変更することが可能である。

**【 0 0 7 1 】**

## [その他の実施の形態]

上述した実施の形態の機能を実現するべく各種のデバイスを動作させるように、該各種デバイスと接続された装置或いはシステム内のコンピュータに対し、上記実施の形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステム或いは装置のコンピュータ（CPU或いはMPU）に格納されたプログラムに従って上記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

## 【0072】

また、この場合、上記ソフトウェアのプログラムコード自体が上述した実施の形態の機能を実現することになり、そのプログラムコード自体は本発明を構成する。そのプログラムコードの伝送媒体としては、プログラム情報を搬送波として伝搬させて供給するためのコンピュータネットワーク（LAN、インターネット等のWAN、無線通信ネットワーク等）システムにおける通信媒体（光ファイバ等の有線回線や無線回線等）を用いることができる。

## 【0073】

さらに、上記プログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記録媒体は本発明を構成する。かかるプログラムコードを記憶する記録媒体としては、例えばフレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、磁気テープ、不揮発性のメモリカード、ROM等を用いることができる。

## 【0074】

また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施の形態の機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているOS（オペレーティングシステム）或いは他のアプリケーションソフト等と共同して上述の実施の形態の機能が実現される場合にもかかるプログラムコードは本発明の実施の形態に含まれることはいうまでもない。

## 【0075】

さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコン

コンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるCPU等が実際の処理の一部又は全部を行い、その処理によって上述した実施の形態の機能が実現される場合にも本発明に含まれることはいうまでもない。

#### 【0076】

なお、上記実施の形態において示した各部の形状及び構造は、何れも本発明を実施するにあたっての具体化のほんの一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、又はその主要な特徴から逸脱することなく、様々な形で実施することができる。

#### 【0077】

##### 【発明の効果】

以上のように本発明によれば、改変ありと判定された画像ファイルの付属情報の表示形態を変更することができるので、改変されている可能性のある画像ファイルの付属情報を検証者にわかり易く通知することができる。

##### 【図面の簡単な説明】

##### 【図1】

第1の実施の形態における画像検証システムの主要な構成要素を示す図である。

##### 【図2】

MAC付き画像ファイルの生成処理を説明するためのフローチャートである。

##### 【図3】

デジタル署名付き画像ファイルの生成処理を説明するためのフローチャートである。

##### 【図4】

MAC付き画像ファイルの構成の一例を示す図である。

##### 【図5】

デジタル署名付き画像ファイルの構成の一例を示す図である。

##### 【図6】



画像検証装置 2 0 の主要な構成要素を示す図である。

【図 7】

画像登録処理を説明するためのフローチャートである。

【図 8】

”MAC”グループの一覧画面（検証前）の一例を示す図である。

【図 9】

”デジタル署名”グループの一覧画面（検証前）の一例を示す図である。

【図 1 0】

第 1 の画像検証処理を説明するためのフローチャートである。

【図 1 1】

第 2 の画像検証処理を説明するためのフローチャートである。

【図 1 2】

”MAC”グループの一覧画面（検証後）の一例を示す図である。

【図 1 3】

”デジタル署名”グループの一覧画面（検証後）の一例を示す図である。

【符号の説明】

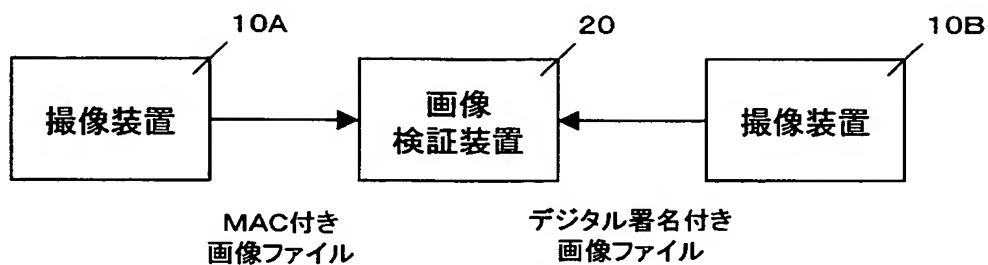
1 0 A 撮像装置

1 0 B 撮像装置

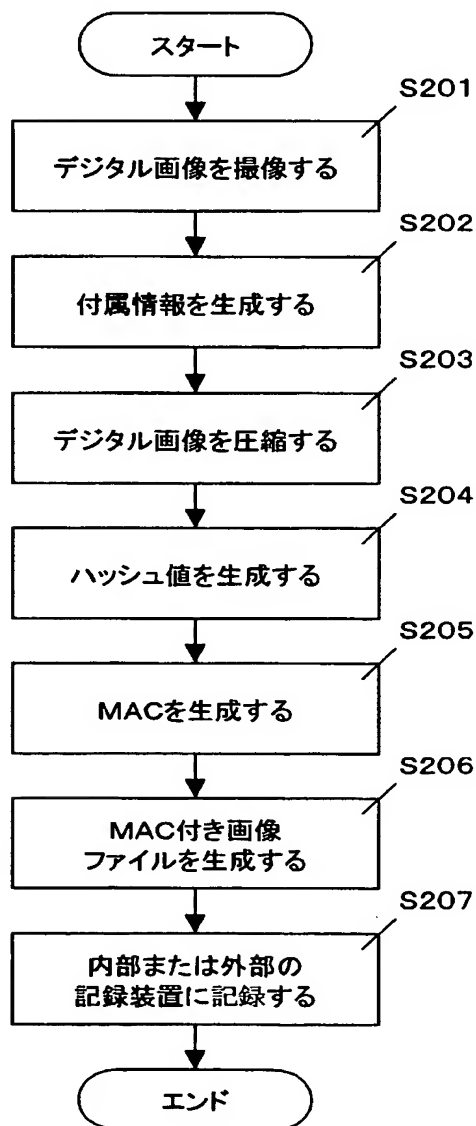
2 0 画像検証装置

【書類名】 図面

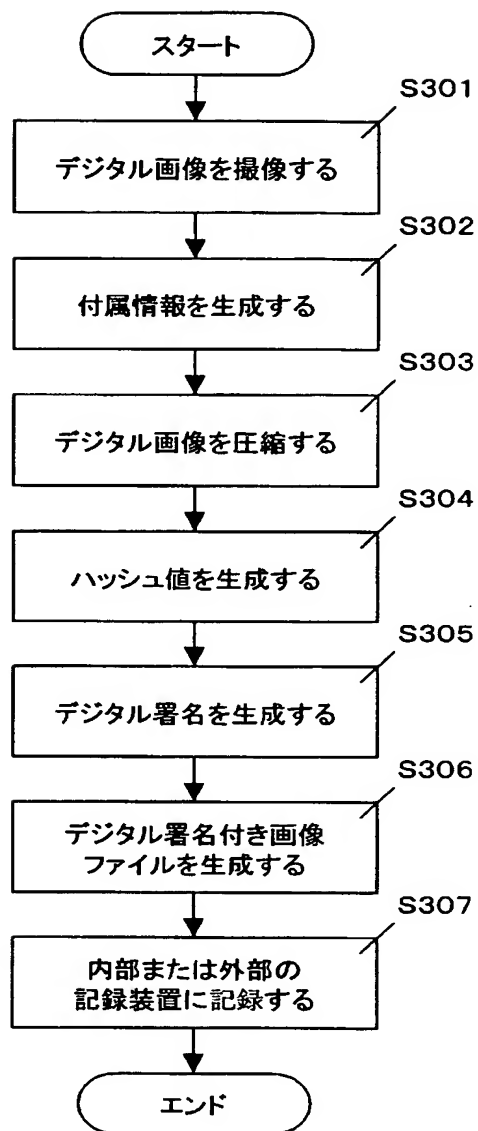
【図 1】



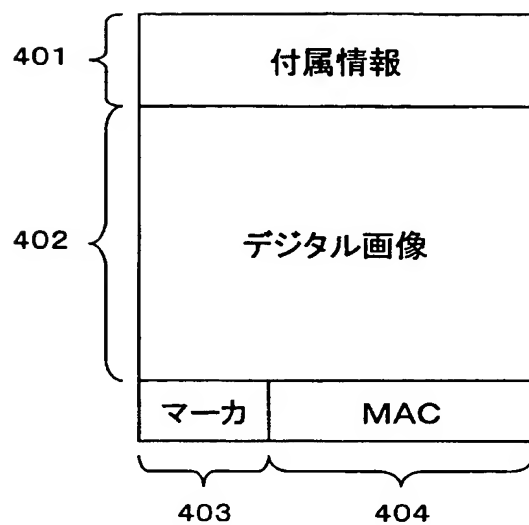
【図 2】



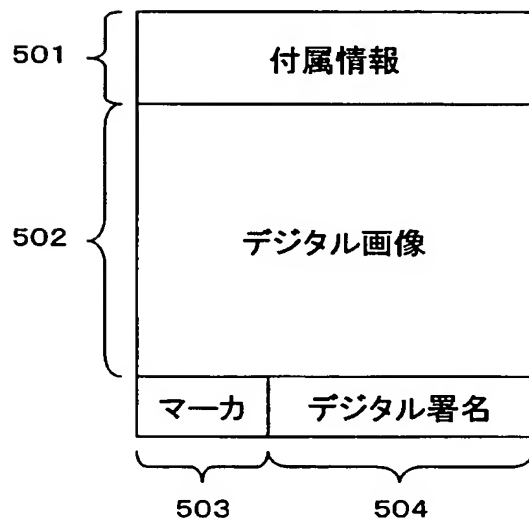
【図 3】



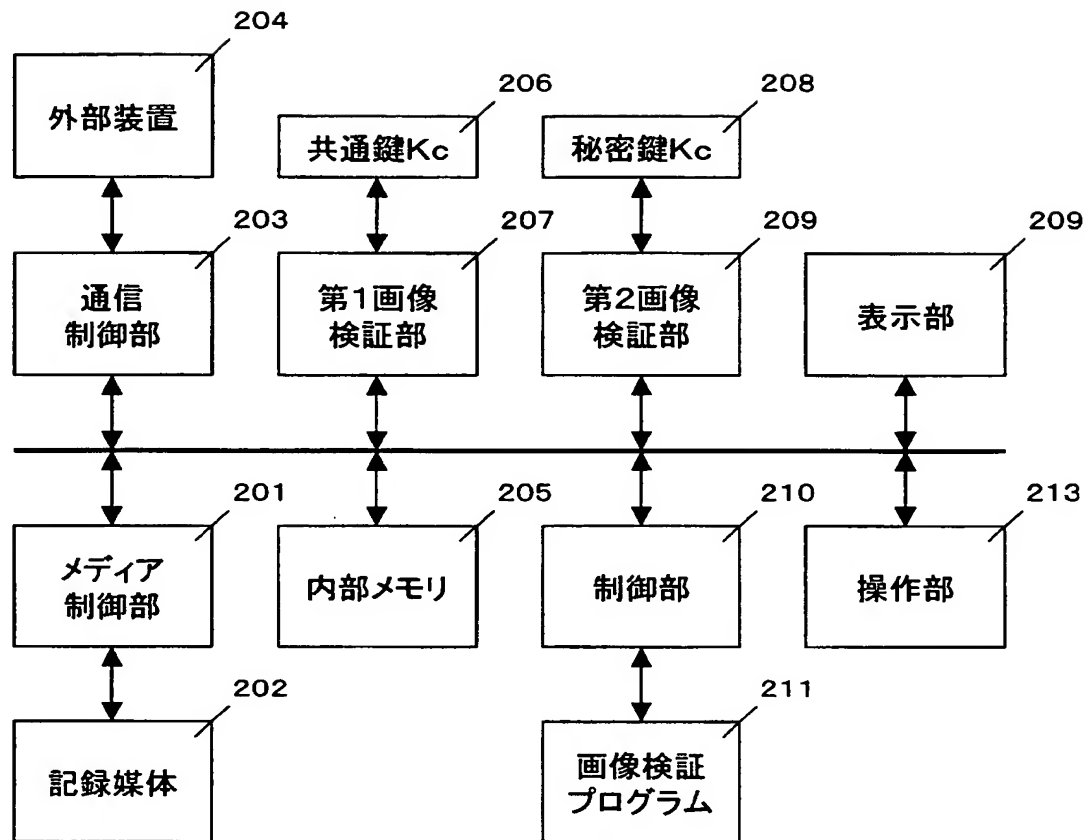
【図 4】



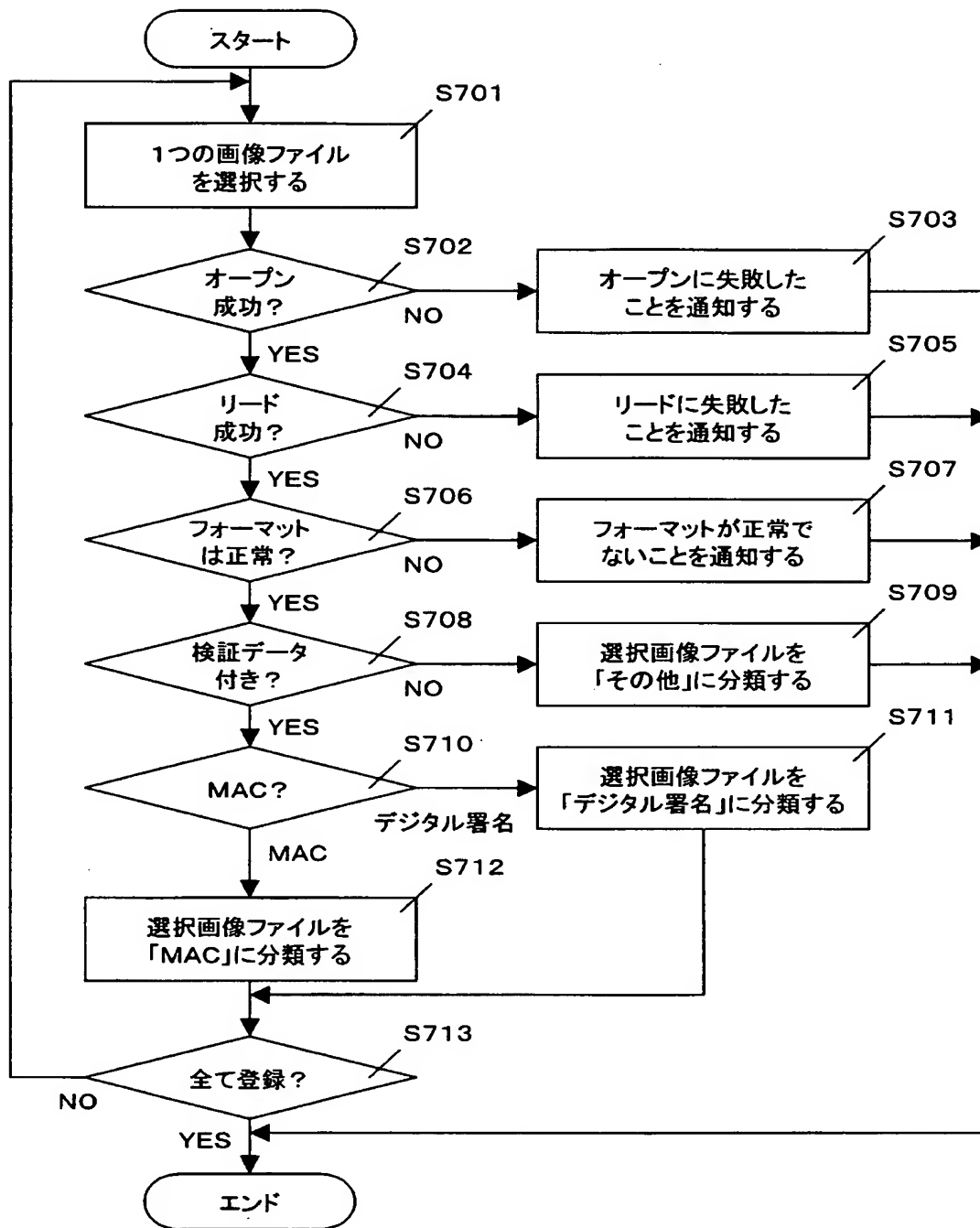
【図 5】






【図 6】



【図 7】






【図 8】

MAC(10)									
デジタル署名(7)		その他(3)							
サムネイル	ファイル名	撮影日	シャッター速度	絞り値	ISO感度	サイズ	モデル名	カメラID	検証結果
	IMG_0001.JPG	2002.12.01 10:40:17	1/800	5.6	100	1M	EOS XX	FE0001	
	IMG_0002.TIF	2002.12.01 10:43:32	1/800	5.6	100	2M	EOS XX	FE0001	
	IMG_0003.JPG	2002.12.01 10:46:12	1/1000	5.6	400	8M	EOS XX	FE0001	
:	:	:	:	:	:	:	:	:	:
:	:	:	:	:	:	:	:	:	:

総ファイル数: 20

検証開始

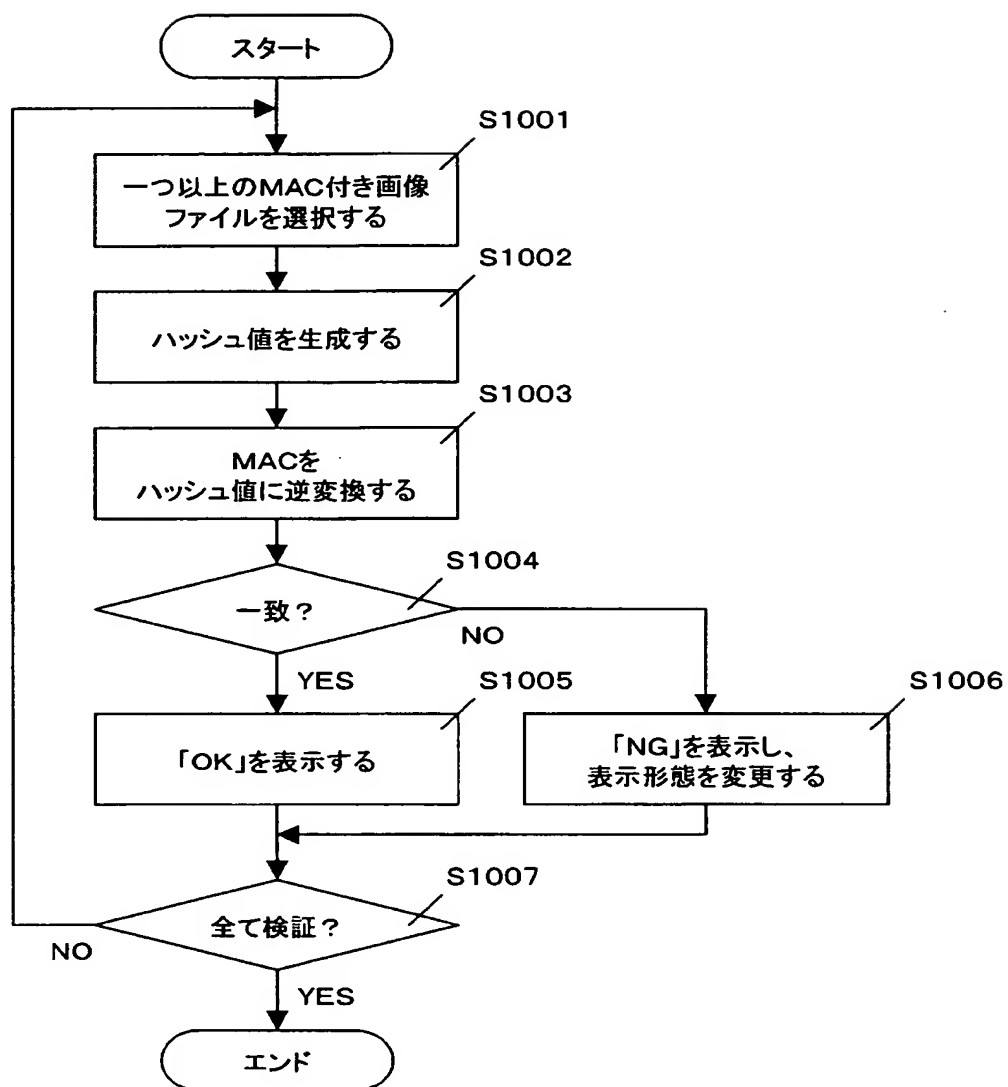
【図 9】

MAC(10)									
デジタル署名(7)		その他(3)							
サムネイル	ファイル名	撮影日	シャッター速度	絞り値	ISO感度	サイズ	モデル名	カメラID	検証結果
	IMG_0021.JPG	2002.12.11 13:43:27	1/800	5.6	100	1M	EOS XX	FE0001	
	IMG_0022.TIF	2002.12.11 13:43:32	1/800	5.6	100	2M	EOS XX	FE0001	
	IMG_0023.JPG	2002.12.11 13:46:36	1/1000	5.6	400	8M	EOS XX	FE0001	
:	:	:	:	:	:	:	:	:	:
:	:	:	:	:	:	:	:	:	:

総ファイル数: 20

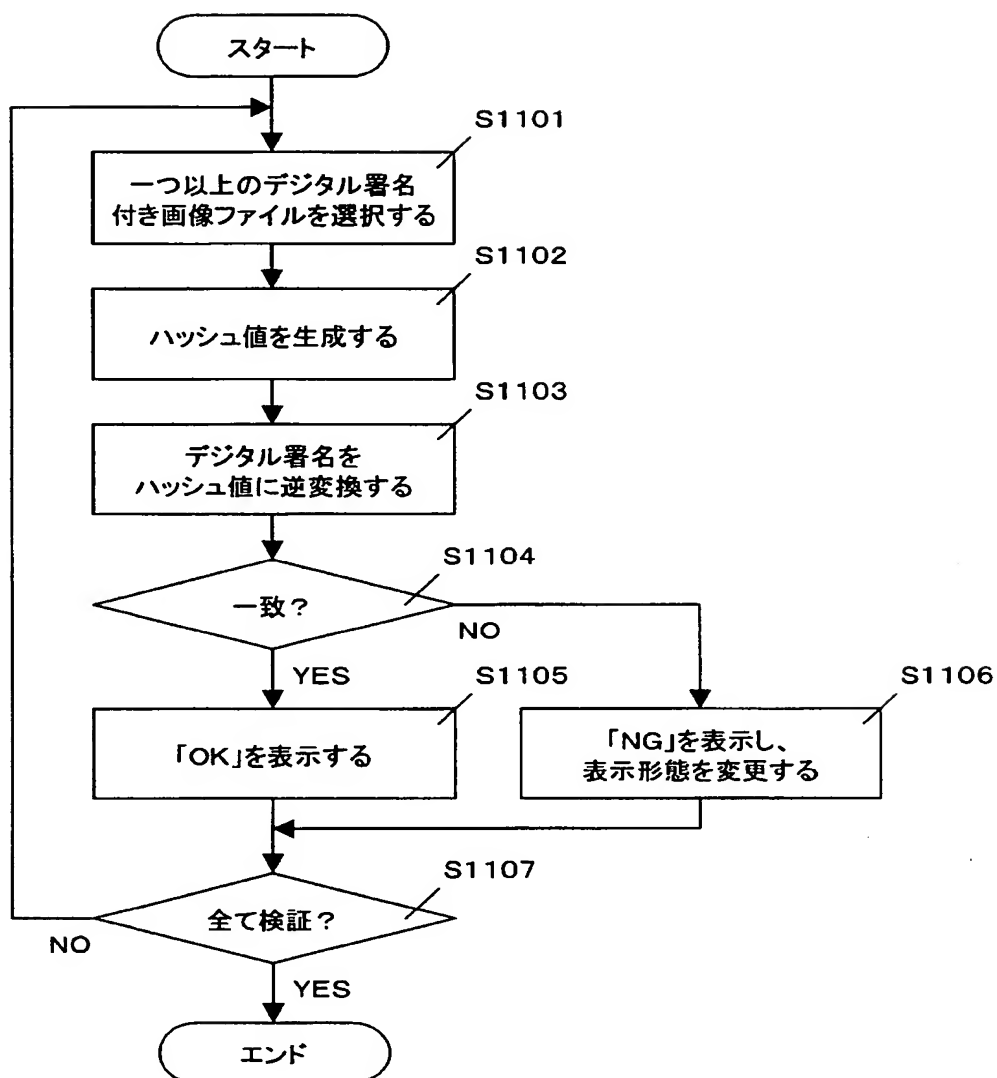
検証開始

【図10】








【図 11】






【図 12】

MAC(10) デジタル署名(7) その他(3)									
サムネイル	ファイル名	撮影日	シャッター速度	絞り値	ISO感度	サイズ	モデル名	カメラID	検証結果
	IMG_0001.JPG	2002.12.01 10:40:17	1/800	5.6	100	1M	EOS XX	FE0001	OK
	IMG_0002.TIF								NG
	IMG_0003.JPG	2002.12.01 10:46:12	1/1000	5.6	400	8M	EOS XX	FE0001	OK
:	:	:	:	:	:	:	:	:	:
:	:	:	:	:	:	:	:	:	:

総ファイル数: 20

検証開始

【図 13】

MAC(10) デジタル署名(7) その他(3)									
サムネイル	ファイル名	撮影日	シャッター速度	絞り値	ISO感度	サイズ	モデル名	カメラID	検証結果
	IMG_0021.JPG	2002.12.11 13:43:27	1/800	5.6	100	1M	EOS XX	FE0001	OK
	IMG_0022.TIF								NG
	IMG_0023.JPG	2002.12.11 13:48:38	1/1000	5.6	400	8M	EOS XX	FE0001	OK
:	:	:	:	:	:	:	:	:	:
:	:	:	:	:	:	:	:	:	:

総ファイル数: 20

検証開始

【書類名】 要約書

【要約】

【課題】 改変されている可能性のある付属情報を検証者にわかり易く通知できるようにする。

【解決手段】 画像検証装置 2 0 は、撮像装置 1 0 A で生成された M A C 付き画像ファイル又は撮像装置 1 0 B で生成されたデジタル署名付き画像ファイルが改変されているか否かを検証する機能と、検証した結果を検証者に通知する機能とを有する装置である。また、画像検証装置 2 0 は、M A C 付き画像ファイル又はデジタル署名付き画像ファイルの付属情報（サムネイル画像、撮影日時、シャッター速度、絞り値、I S O 感度、モデル名、製造番号など）を検証者に通知する機能を有する装置でもある。

【選択図】 図 1

特願 2 0 0 3 - 1 0 2 3 2 7

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 1 0 0 7 ]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都大田区下丸子 3 丁目 3 0 番 2 号

氏 名

キャノン株式会社